



Rotterdam Port
Cyber Resilience

NIEUWE STAP IN CYBERWEERBAARHEID

OKTT-STATUS VOOR FERM

ROTTERDAM, 19 MEI | Stichting FERM heeft vanuit het partnerschap met het Nationaal Cyber Security Centrum (NCSC) de OKTT-status toegewezen gekregen. Het NCSC kan vanuit zijn wettelijke grondslag alleen informatie over dreigingen en incidenten delen met een samenwerkingsverband dat **objectief kenbaar tot taak (OKTT)** heeft andere organisaties of het publiek te informeren. Dankzij de toekenning van de OKTT-status kan FERM voorzien in tijdige, actuele en relevante dreigingsinformatie in het nieuwe IT-portal voor participanten, waarin informatiedeling centraal staat.

De vernauwde samenwerking die FERM aangaat met zowel het NCSC als de NCTV is een belangrijke stap in de cyberweerbaarheid van de aangesloten organisaties in de haven.

“Nu we de OKTT-status hebben, kunnen we onze participanten nog beter helpen”, zegt FERM-directeur Evelien Bras. “Met hulp van het NCSC kunnen we hele specifieke dreigingsinformatie met hen delen, waardoor we weer een stapje verder kunnen gaan in het cyberweerbaar maken van het Haven Industrieel Complex. Dit is een echte meerwaarde voor alle bedrijven in de Rotterdamse Haven, zeker nu we gelukkig zien dat steeds meer bedrijven zich bij ons aansluiten.”

“Het proces van informatieverspreiding begint wanneer er een bericht wordt verzonden vanuit het NCSC over een mogelijke dreiging. Dat bericht komt terecht bij de aangesloten organisaties. Mocht het gaan om een dreiging met (mogelijke) impact, dan kan het door de OKTT's worden gedeeld met aangesloten partijen – in dit geval de participanten die aangesloten zijn op het IT-portal van FERM.”

Samenwerking NCSC

“Cybersecurity incidenten, kwetsbaarheden en dreigingen kunnen grote gevolgen hebben”, zo licht NCSC-directeur Hans de Vries de keuze toe. “Neem bijvoorbeeld de problemen met Citrix vorig jaar of recenter de Microsoft Exchange Servers: als de IP-adressen van de bedrijven die bij FERM aangesloten zijn in onze systemen zitten, kunnen wij FERM relevante informatie dreigings- en risico-informatie sturen in relatie tot die IP-adressen die zij kunnen doordelen met hun achterban.”

“Zo zijn ransomware aanvallen de laatste tijd aan de orde van de dag. Bij een geslaagde aanval heeft een kwaadwillende toegang tot de IT-systemen van het bedrijf, wat de beschikbaarheid van systemen en de integriteit en vertrouwelijkheid van data in gevaar brengt. Criminelen gooien hun ‘net’ vaak breed uit. Dan helpt het als je als bedrijf snel informatie hebt over hoe actiegroepen te werk gaan, om na te gaan of je eventueel kwetsbaar of geraakt bent zodat je zo snel mogelijk (voorzorgs)maatregelen kunt treffen.”



Rotterdam Port
Cyber Resilience

“In de Rotterdamse Haven komt daar bovenop dat bedrijven zoals containerterminals en rederijen onderling veel data uitwisselen. Als daarin iets misgaat, krijg je een domino-effect, waardoor alles stil komt te liggen. Dus ook op het gebied van cyber sta je samen FERM.”

Aanmelden voor FERM

Cybersecurity kun je samen effectief aanpakken, met de nabije collega-bedrijven die je vertrouwt. Zo weet je wat er speelt in jouw omgeving, en waar je op moet letten. FERM zorgt voor dreigingsbeelden, voorziet in crisisoefeningen en werkt samen met onder andere Havenbedrijf, politie en justitie, het ministerie van Economische Zaken en het NCSC om óók de havenspecifieke dreigingen – zoals storage spoofing – aan te pakken.

FERM is er voor alle organisaties in het sterk verbonden netwerk van ruim 700 bedrijven in het Haven Industrieel Complex, met ondersteuning en dienstverlening voor klein-, midden- en grootbedrijf. Kijk voor meer informatie op ferm-rotterdam.nl/participant-woorden.

Voor meer informatie

FERM Rotterdam

Evelien Bras

E-mail: evelien.bras@ferm-rotterdam.nl

Tel: 06 – 388 29 965

Over FERM

Stevig, standvastig en sterk. FERM is geen afkorting, maar de Rotterdamse vertaling van resilience. FERM brengt bedrijven en kennis bij elkaar en faciliteert het onderling uitwisselen van dreigingsinformatie, oplossingen en best-practices. Het organiseert gezamenlijke trainingen zodat ook jouw personeel bij blijft met de laatste ontwikkelingen en weet wat hun te doen staat. Ook brengt FERM samen met de achterban kwetsbaarheden in kaart, zodat je kan acteren op de laatste stand van zaken.

FERM Rotterdam is ontstaan als onderdeel van het Port Cyber Resilience Programma. Doel van het programma is het stimuleren van samenwerking tussen bedrijven in de Rotterdamse Haven en het verhogen van het bewustzijn met betrekking tot cyberrisico's om zo de best digitaal beveiligde haven van de wereld te worden.

Een cyberaanval op een bedrijf in de Rotterdamse Haven heeft vrijwel zeker ook negatieve gevolgen voor andere organisaties binnen de keten. We sterk afhankelijk van elkaar, en onze processen zijn met elkaar verbonden. We zijn bovendien vrijwel allemaal afhankelijk van onze informatietechnologie (IT) en operationele technologie (OT). Dat biedt geweldige economische kansen, maar het maakt ons ook kwetsbaar. Een kwetsbaarheid waar we gezamenlijk in op kunnen treden. | www.ferm-rotterdam.nl